REMARKS

Claims 12-36 and 39-63 remain in this application. Of the pending claims, claims 12-14, 34-36, 39-41 and 61-63 are independent. None of the claims have been amended in this response.

Claims 12-36 and 39-63 were rejected under 35 U.S.C. §102(e) as being clearly anticipated by *Barnett et al.* (US Patent 6,321,208). Applicant traverses these rejections. Favorable reconsideration is respectfully requested.

Specifically, *Barnett* does not disclose a client computer configured for, or the step of, transmitting an order acceptance request over a packet-switched network that includes a plurality of modular elements, with each modular element individually protected by an imbedded cryptographic security code, as recited in claims 12-14, 34-36, 39-41 and 61-63. Also among the features of the pending claims is a server configured to, or the step of, transmitting an order acceptance response to a client, the order acceptance response also including a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element.

Barnett discloses a method and system for the electronic distribution of product redemption coupons to remote personal computers located at users' homes. A web site stores packages of coupon data for downloading on demand to the user's computer, where the user may view, select, sort and print desired coupons from the downloaded package (see Abstract, col. 4, lines 40-60). The user's demographic as well as coupon selection data is then provided back to the web site and coupon distributor and issuers for subsequent marketing analysis and the distributors/issuers can also determine how many times a particular coupon was viewed or downloaded (col. 5, lines 22-33).

When obtaining coupons under *Barnett*, a remote personal computer 6 is connected to a printer 8, that is instructed by the coupon data management routines 32 stored in the computer 6 in order to print coupons 18. Once printed, the coupons 18 are used in the normal fashion by a consumer when shopping at a desired retail store 10. In other words, the coupons 18 are presented to a product checkout station 11 along with the associated products for purchase, and the discount amount shown on the coupon 18 is credited to the consumer at the point of sale (col. 7, lines 6-17). According to *Barnett*, the coupons 18 contain user-specific data in the form of a unique user bar code 90, as shown graphically in FIG. 5. The user bar code 90 is encoded with user-specific information such as the user name and/or other unique identification criteria such as a social security number or online service address (col. 7, lines 21-35).

Applicants submit that the barcode encoding is wholly irrelevant to the cryptographic encoding recited and disclosed in the present application. For one, the system and underlying technology of bar-coding is premised upon *symbology*, which deals with encoding digits/characters of a message, as well as the start and stop markers, into bars and space. The symbology of the barcode (e.g., UPC, code 128, etc.) is merely a machine-readable representation of information in a visual format on the physical surface of a coupon (such as ref. 90 of *Barnett*). The representation is subsequently read by a fixed-light or laser scanner, which sweeps a beam of light across the barcode in a straight line, reading a slice of the barcode light-dark patterns to obtain the information. Thus, *Barnett* teaches the use of barcoding to provide a unique identity information to each coupon (e.g., user information, expiration date), where the coupon redemption center may control the time (i.e., before an expiration date) or manner (i.e., only one coupon redemption per user) in which the coupon is redeemed based on this identity information (see col. 11, lines 2-23).

In contrast, the present invention recites *cryptography* in the form of security codes embedded within each of the plurality of modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon. As is known in the art, cryptography deals with the secure encoding and authentication of the data itself. In the present application, the present specification describes, as an example, the use of key authentication, such as SSL, which contain cryptographic protocols which provide secure communications on the Internet (page 9, lines 6-29; see also page 19, lines 21-28). Under the example of SSL, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated. For mutual authentication, clients must be provided with public key infrastructure (PKI) deployment. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery during the transmission and recept of a commercial transaction that occurs over the Internet. Claims 35 and 62 specifically recite the use of digital signatures, and claims 36 and 63 specifically recite the use of message authentication codes.

This is neither taught nor suggested in *Barnett* – as discussed above, *Barnett's* system does not conduct commercial transactions over the Internet using the coupons; the entire disclosure is premised entirely on the user printing and physically redeeming the coupon at a retail store or coupon redemption center through the use of barcode scanning. *Barnett* briefly mentions that coupons may be redeemed "electronically" (see FIG. 9, col. 11, lines 29-42), however, it is clear from the disclosure that the "electronic" redeeming of coupons involves the transmission and storage of the coupon at the retail center, where the retail center prints and scans the coupon on location ("[t]hus, the printable coupon data generation routine ***32d*** combines all this information and generates a record indicative of the unique coupon to be printed"). Even if *Barnett* used technology such as PKI certificates, the entire purpose of such coding would be lost upon subsequent barcoding of the user information.

As *Barnett* does not conduct transactions of the products underlying the printed coupons, *Barnett* also fails to teach or suggest the processing and negotiatiation of electronically authenticated coupons. The present claims recite that the order acceptance request is authenticated and processed to contain a discreet message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements. *Barnett* is completely silent as to how each of the user information is individually protected through the use of barcodes.

Also, claims 12 and 39 recite that the client computer is programmed to receive the digital coupon, protected by a cryptographic security code, "from another computer." Claims 13 and 40 further recite that the authenticated coupons are accepted "without regard to the identity of the coupon holder." These elements are clearly not taught or suggested in the disclosure of *Barnett*.

In light of the above amendments and arguments, Applicants submit that claims 12-36 and 39-63 are allowable. Applicants respectfully submit that the patent application is in condition for allowance and request a Notice of Allowance be issued. The Commissioner is authorized to charge and credit Deposit Account No. 02-1818 for any additional fees associated with the submission of this Response. Please reference docket number 0115274-0008.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY ____________________
Peter Zura
Reg. No. 48,196
Customer No. 24573
Phone: (312) 807-4208

Dated: March 29, 2006